A New Approach for Detecting and Monitoring of Selective Forwarding Attack in Wireless Sensor Networks

Naser M. Alajmi and Khaled Elleithy
Computer Science and Engineering Department
University of Bridgeport
Bridgeport, CT, USA
nalajmi@my.bridgeport.edu , elleithy@bridgeport.edu

***Abstract*— Wireless sensor networks (WSNs) are susceptible to most security attacks. There are some limitations such as reliability, energy efficiency, and scalability, which affect sensor nodes. These limitations mostly affect the security of wireless networks. Also, limited capacity of sensor nodes accounts for the security attacks on WSNs. Applications such as military surveillance, traffic surveillance, healthcare, and environmental monitoring are impacted by security attacks. Hence, researchers have created various types of detection approaches against such attacks. Selective forwarding attack is an example of an attack that is not easily detected particularly in the networks layer. In this type of attack, malicious nodes function in the same way as other nodes in the networks. However, it tries to drops the sensitive information prior to transferring the packet to other sensor node. In this paper, we proposed a new approach for detecting and monitoring selective forwarding attacks in wireless sensor networks. The new approach guaranteed to keep the data transferring between nodes safely.**

Keywords*— *Wireless Sensor Networks (WSNs) and Selective Forwarding Attacks.

I. INTRODUCTION

The challenges in the network layer are limited memory, buffering, and saving power. Hence, these challenges are impacted to the WSNs. Routing is the major function in this layer. Network layer is subjected many routing protocols for instance, Flat routing, and hierarchal routing. The simple function of the routing protocol is to find the reliability path. Data aggregation is used in flat routing. It a set of automated methods combining the data that comes from sensor nodes into a set of relevant information and exclude the duplication [1]. LEACH is a popular hierarchy routing protocol [2]. It separates the network into clusters and randomly and selects the cluster head to do the routing function from cluster to the base station. A network layer in WSNs is subjected to many types of attacks. Furthermore, a sensor node may acquire advantages of multi-hop by simply refusing to route packets. Therefore, it could be executed all the time with the net result. If a neighboring node marks a route through the malicious node, then it will be unable to modify messages [3]. There are assortments of attacks targeting the network layer. The attacker can attack the routing protocol by injecting the path between the source and the base station.

Sensors, ad hoc, mobile, and wireless are properties merged together in networks. They are a wide assortment of implementations in the real world. These implementations are for instance, monitoring factory environments, and energy emergency response information [4]. The sensor networks susceptible different types of security threats from attackers at most layers of the networks. Network layer is the important layer in the networks and prone many types of security attacks. The most attacks in sensor network routing are spoofing, selective forwarding, sinkhole, Sybil attack, wormhole attack, node replication attack, flooding and attack against privacy. Selective forwarding attack is the type of attack that we focus on it. It is an insider attacks and the adversaries are able to create routing loops that attract or repeal network traffic. Also, they can extend or shorten source routers, generate false messages, and attempt to drop the significant messages. The drop packets come from one node or a set of nodes. A malicious node refuses to forward the messages or drop packets randomly [4]. The positions of the nodes do not need to be predetermined. Sensor nodes are deployed in high-risk areas. The majority of WSN protocols do not have the security to prevent simple attacks on the nodes [5]. Thus, sensor network protocol and algorithms should be self-organizing. Some design factors exist for sensor networks and sensor nodes. These factors are significant in the design of protocols or algorithms. The impact of these factors can be used to compare different approaches [6]. The factors include scalability, fault tolerance, network topology, power consumption, production cost, hardware constraints, environment, and transmission media.

The features of sensor nodes guarantee many applications. The rapid deployment, self-organization, and fault tolerance can provide a promising sensing method for certain functions, such as control, communication, and computing [7], [8]. Networks have different applications. Therefore, applications comprise several levels of monitoring, tracking, and controlling. A group of applications is employed for specific purposes. In military applications, sensor nodes include monitoring, battlefield surveillance and object tracking. The battlefield monitors utilized in military operations have prompted the development of WSNs. In medical applications, sensors aid in patient diagnosis and monitoring. The majority of these applications are deployed to monitor an area and react when a sensitive factor is recorded [9].

II. Selective Forwarding Attacks

Sensor nodes use communication to transfer packets from the source to base station by using multi-hop. In selective forwarding attack, malicious nodes have attempted to stop the packets in a network by rejecting message forwarding. It is not easy to detect this type of attack due to unreliable communications. Selective forwarding attacks can be impacted to some routing protocols [1]. It compromised node has notable consequences. A compromised node selectively drops packets. Malicious nodes work in the same manner such as other nodes in the network field. However, these malicious nodes attempt to find sensitive messages and drop them before sending the entire packets to the next nodes. The attacker makes sensor network rely on the redundancy forwarding by using broadcast for data to spread in network. Based on researchers, limited power and low memory are obstacles that make conventional security measures inappropriate for WSNs [2]. The attacker compromises internal sensor nodes then launch attacks, which it is hard to detect it. Sensor node has limited communication and computational resources. It has short radio range and it is simply compromised by an attacker. The attacker can refuse to forward the messages to other nodes or drop sensitive information. For this reason, the base station may not receive the entire message.

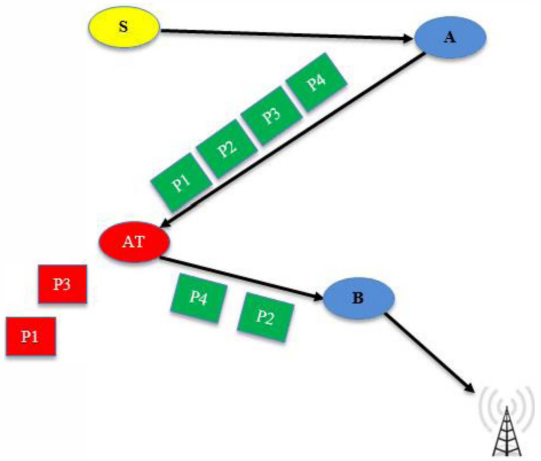

Fig 1. Selective Forwarding Attack-Drop Some Packets

Sensor node has limited communication and computational resources. It has short radio range and it is simply compromised by an attackers. As a result, in figure 1 node A sent some packages (P1, P2, P3, and P4) to node B using the route that is between the two nodes. The attacker breaks the link between nodes and steals two packets (P1 and P3), keep the other packets (P2 and P4) transferred to the base station.

In figure 2, there are two sensor nodes A and B transfer some packets to node C. node A send (P2 and P4) and node B send (P1 and P3). The attacker who breaks the link between nodes drop the two packets that sent from node A so the entire packet is not transferred to the base station. However, the other two packets that sent from node B were transferred to node C.

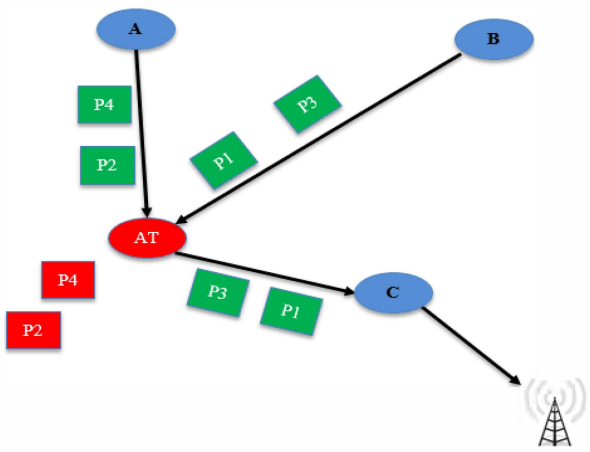

Fig 2. Selective Forwarding Attack-Drop Entire Packets

III. Related Works

Yu and Xiao [10] proposed an approach based on lightweight security to detect a selective forwarding attack in the environment of sensor networks. The approach utilized a multi-hop acknowledgment to launch alarms by obtaining responses from the nodes that are located in the middle of paths. Authors assumed the approach could identify malicious sensor nodes. The aim of the detection attack is to send an alarm when a malicious node is discovered, which indicates a selective forwarding attack. Yu and Xiao employed two detection processes in the scheme which are downstream process and upstream. A report packet is created and sent to the base station hop by hop when nodes detect a malicious node. Therefore, the base station would receive the alarm packet and forward multiple hops that are produced by the node. An acknowledgement packet and an alert packet will drain the energy during detection.

Tran Hoang and Eui-Nam [11] proposed an approach against selective forwarding attacks that consists of a lightweight detection mechanism. The detection is a centralized cluster, which utilized the two-hop neighborhood node information and overhearing technique. It is dependent on the broadcast nature of sensor communication and the high density of sensors. Each sensor node is provided with a detection module that is constructed on an application layer. Sensor node sets routing rules and two-hop neighbor knowledge to generate an alert packet. Hoang and Nam suggested that the two routing rules make the monitoring system more suitable. Thus, the first rule is to determine if the destination node forwards the packet along the path to the sink. When the malicious counter crossed the threshold X, it revoked the malicious node from its neighbor list.

Huijuan Deng et al, [12] proposed an approach to secure the data transmission and detecting a selective forwarding attack. They used watermark technology to detect malicious nodes. Prior to employing a watermark technique, they used a trust value to determine a source path for message forwarding. The trust value involves weighting the credit of each sensor node. They assumed that the base station is always trustworthy and cannot be comprised by the adversary, which renders the scheme inappropriate for real wireless sensor networks. Every

node has a trust value. At the beginning of network initializing, all nodes should have the same trust value. Huijuan Deng et al. utilized the watermark technique to calculate the packet loss. Data transmission begins when an optimal routing path is confirmed. The base station creates a κ bits binary sequence as the original watermark message. Therefore, a watermark message is part of the packets. A base station compares the extract watermark to the original watermark to detect a selective forwarding attack.

Chanatip et al. [13] have proposed a lightweight approach. They used Extra Monitor (EM) to eavesdrop and monitor all traffic when transferring data between nodes. They also employed RSSI to detect a sinkhole attack. The value of RSSI is that four EM nodes can be arranged to establish the positions of all sensor nodes, of which the base station position should be (0, 0). Chanatip et al. have assumed that the network is static when sensor nodes are deployed; thus, any change in the type of topology will immediately affect their approach. They assumed that the attackers could capture and damage the nodes. Therefore, all sensor nodes must protect or use tamper robust hardware.

IV. Proposed System

In wireless sensor network, several nodes transfer sensor readings to the base station to process data. Military bases might find the importance of using sensor networks in order to explore enemy forces. Sensor nodes have limited sensing and computation. Also, nodes have communication ability. Sensor readings collect data when it detects unusual activities of enemy forces such as warplanes, and war tanks movement in battlefields. Data will be sent to the base station through routers. In military applications, selective forwarding attacks destroy the transmission packets between the source and base station, and sometimes between the sensor nodes. Malicious nodes refuse to transfer an entire packet. It drops the sensitive information and then forwards the remaining packet.

We designed three layers including MAC pool IDs layer, rule-based processing layer, and anomaly detection layer. They maintain the safety of data transmission between a source node and base station while detecting selective forwarding attacks. Furthermore. We demonstrate the performance of the protocol by creating a military base scenario. It is simulated using Network Simulation-2 NS2. There are some assumptions to detect the selective forwarding attack within certain applications. We assume that all nodes are the same specification. All nodes in the network are having the same energy at starting point and having maximum energy. As well as, we assume that nodes are uniformly distributed in network in a random manner. Malicious nodes should not drop any packets before launching a selective forwarding attack, and an adversary cannot attack nodes during their deployment. Nodes can send data to Base station. Received Signal Strength Indicator-RSSI is the mechanism to measure the distance between the base station and node.

The new approach finds a secure route during the data transmission. We assumed, Wireless sensor networks are complicated. In order to create a simple solution to detect the selective forwarding attack, we have made some assumptions for the approach detection within significant applications that are susceptible in networks. These assumptions should be acceptable in the sensor networks. First of all, we assume that secured communication should be part of the networks. Second, Malicious nodes should not drop any packets prior to the launching of the selective forwarding attack. Third, we assume that the adversary cannot compromise a sensor node during the deployment. Finally, we assume that authentication broadcast protocols were applied to each sensor node.

A. Selective Forwarding Detection and Monitoring Approach

In wireless sensor networks, the rule-based intrusion detection system (IDS) is one of the mechanisms for protection against the security attacks. Rule-based IDS are known as signature-based IDS. The network layer in WSNs is threatened via some attacks such as a wormhole attack, a sinkhole attack and other types of attacks. Our proposal focuses on the selective forwarding attack. We design multi layer approach, which includes three security layers depicted in Figure 3. The first layer is data receiving. In this layer, the important information is filtered and stored. The information includes message fields that are useful to the rule processing. The second layer is rule processing. In this section, rules must be applied to the stored data. The message can be rejected or refused. In addition, no rules will be applied to the message since it fails. The third layer is detection. The detection approach saves energy by using low memory and it takes not much time. It chooses a secure route to transfer data between the source and the base station. Furthermore, SFD approach is reliable, energy efficient, and scalable. All these factors are significant for the sensor nodes. Our approach assumes that the detection accuracy is high, even though the radio condition is poor.

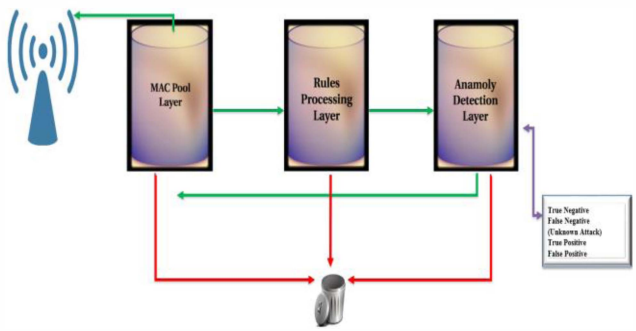

Fig 3. Selective Forwarding Detection-Multi-Layers

B. System Model

The goal of this model is to extend the network life time while maintaining the Quality of Service (QoS). The network lifetime is very important metrics of wireless sensor networks. The model also aims to make a balance for the energy utilization therefore, provide longer secure surveillance for the military application.

B.1. Reliability

In order to develop the reliable communication, we have to determine the reliable path from the sender node to the base station, as the $'\forall K'$ number of the sensor nodes in the reliable optimal $'RP'$ path

$$\prod_{i=0}^{\forall K} RP_{ij} \quad (1)$$

Obtained using Bellman-Ford algorithm's link measurement properties

$$BF = \frac{\theta {\sigma_y}^2}{T_r {d_x}^{-n}} \quad (2)$$

We start searching the reliable path for communication then apply Rayleigh fading model to confirm the reliable communication:

$$RP : RP_{min} \sum_{(i,j \in RP)}^{N} -log \frac{1}{RP_{ij}} - RP_{min} \sum_{(i,j \in RP)}^{N} -log^2$$

$$-(BF) - \sum_{(i,j \in RP)}^{N} (-BF) \quad (3)$$

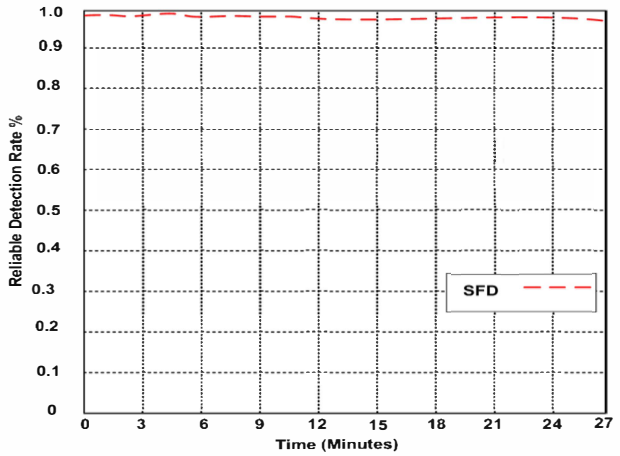

Fig 4. Reliable Detection Rate of SFD Approach

B.2. Energy efficiency

In energy efficiency, we got the differences between the node's individual energy consumption, after defined the total consumed energy for all nodes in the network. Also, determine the average energy consumption of each sensor node, and energy consumed for transmitting the packet and for receiving the packet.

$$\Delta E_a = \sum_{k=0}^{n} k(\Delta E_m) \quad (4)$$

Once, an average energy ΔE_a consumption is determined; then we substitute the minimal energy consumption ΔE_m of each sensor node is calculated in equation,

$$\Delta E_m = \Delta \beta_t \prod_{u \in S(k)}^{n} Y_{uk} + \Delta \gamma_r \prod_{v \in S(k)}^{n} Z_{vk}$$

$$\Delta E_a = \sum_{k=0}^{n} k \left(\Delta \beta_t \prod_{u \in S(k)}^{n} Y_{uk} + \Delta \gamma_r \prod_{v \in S(k)}^{n} Z_{vk} \right) \quad (5)$$

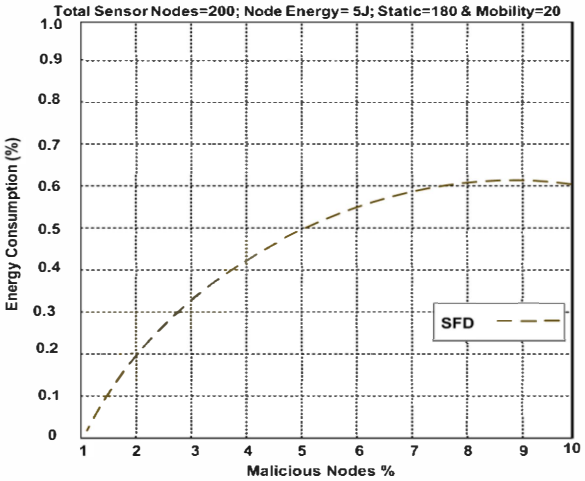

Fig 5. Energy Consumption of SFD Approach

B.3 . Scalability

Scalable probability of network can be defined as:

$$S_p{}^{+} = \sum_{k=0}^{\infty} (k_t) + k_j \times \iint_{i=0\,\&\,j=0}^{N+} (\Delta p)^n + (\nabla p) \quad (6)$$

We can determine the scalable probability of network, once the node wants to leave as:

$$S_p{}^{-} = \sum_{k=0}^{\infty} (k_t) - k_j \times \iint_{i=0\,\&\,j=0}^{N+} (\Delta p)^n - (\nabla p) \quad (7)$$

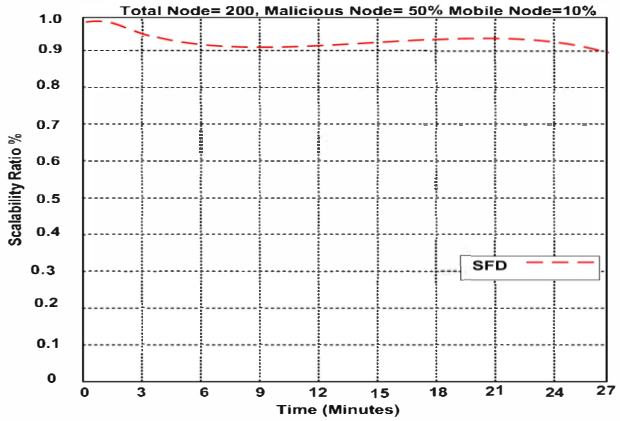

Fig 6. Scalability Ratio of SFD Approach

C. *Results and Discussion*

Approaches are estimated through the simulation. We have pointed on energy consumption, average throughput, reliable detection rate, and scalability ratio. In the simulation, 200 sensor nodes are deployed in an area network size 800 * 800 square meters. Hence, each node has a 35 meters transmission range and sensing range of node is 30 meters. Consequently, the communication overheads are decreased.

Figure 7 describes the detection rate of our approach and other works. We proved our approach with 50% malicious nodes and static nodes. It clearly shows that SFD is stable at almost the same level when the time increased from 0 min to 27 min. Therefore, the new approach is successfully detect the malicious node than others.

In Figure 8, the graph shows our approach with 50% malicious nodes and 50% mobile nodes. It clearly also shows that SFD is stable when the time increased from 0 min to 27 min. Therefore, the new approach is successfully detect the malicious node than others respectively.

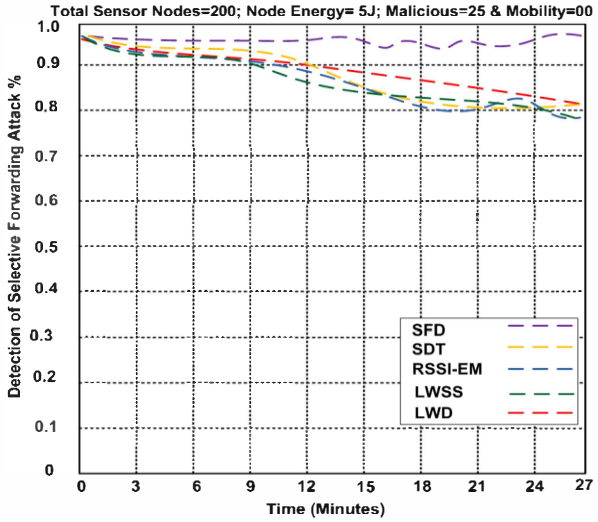

Fig 7. Detection of selective forwarding attack with 50% malicious nodes and static nodes

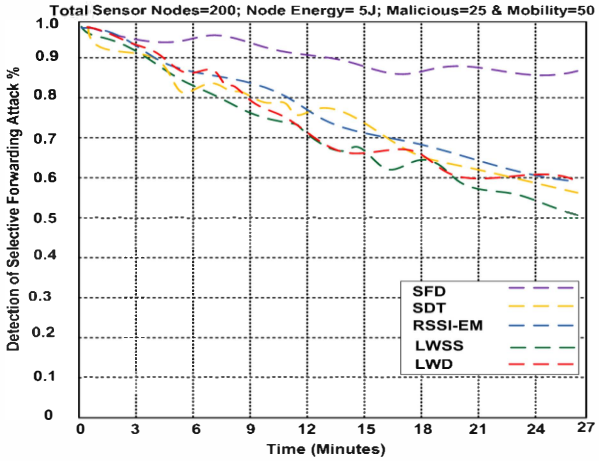

Fig 8. Detection of selective forwarding attack with 50% malicious nodes and 50% mobile nodes

V. CONCLUSION

Selective forwarding detection and monitoring objectives are to detect malicious nodes, extend the network's life time, maintaining the Quality of Service (QoS) based on the three factors which are reliability, energy efficiency, and scalability. The new approach contains of three layers including MAC pool IDs layer, rule-based processing layer, and anomaly detection layer. Selective forwarding detection maintains the safety of data transmission between the source and base station. Also, it improves the performance of attack detection such as in a military application. In addition, the approach is demonstrated using Network Simulation (NS2).

The network's lifetime is most significant metrics of wireless sensor networks. So, we improved reliability detection, reduced the energy consumptions and developed scalability ratio. These factors aim to balance the energy utilization for unevenly distributed sensor nodes and to provide longer secure surveillance for a military base while maintaining the Quality of Service (QoS).

Table1: Benchmark Comparison of Approaches

Approaches	*Bandwidth Consumption*	*Throughput without mobility*	*Throughput with mobility*	*Scalability*	*Accuracy*	*Reliability*	*Packet Delivery rate*	*Detection rate*	*Energy Consumption with mobility*
1. SFD	49.6%	321.2 Kb/Sec	314.6 Kb/Sec	99.1%	98.3%	98.4%	99.2%	97.1%	60.4%
2. LWSS	64.5%	293K b/Sec	297.1Kb/Sec	88.3%	88.9%	88.2%	94.4%	82.1%	75.1%
3. LWD	69.4%	292.9 Kb/Sec	296.8 Kb/Sec	95.1%	90.2%	90.6%	94.1%	80.2%	81.8%
4. SDT	72.3%	278.1 Kb/Sec	277.4Kb/Sec	90%	90.9%	89.6%	94.3%	89.8%	69.1%
5. RSSI-EM	61.2%	292.8 Kb/Sec	296.3Kb/Sec	88.2%	85.6%	86.3%	94.2%	90.1%	68.5%

References

[1] Halawani, S., Khan, A., Sensors Lifetime Enhancement Techniques in Wireless Sensor Networks - A Survey. Journal of Computing, vol. 2, issue 5, May 2010.

[2] Koubaa, A., Alves, M., Tovar , E., Lower Protocol Layers for Wireless Sensor Networks: A Survey. IPP- HURRAY Technical Report, HURRAY-TR-051101. 2005.

[3] J. P. Walters, et al., "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, p. 367, 2007.

[4] Haowen Chan, and Adrian Perrg, "Security and Privacy in Sensor Networks" Carnegie Mellon University pp. 99-101.

[5] Karlof, C. and Wagner, D., "Secure routing in wireless sensor networks: Attacks and countermeasures", Elsevier's Ad Hoc Network Journal, Special Issue on Sensor Network Applications and Protocols, September 2003.

[6] T. Zhu, Z. Zhong, T. He, and Z.-L. Zhang, "Energy-synchronized computing for sustainable sensor networks," *Ad Hoc Networks,* vol. 11, pp. 1392-1404, 2013.

[7] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: remote large-scale environments," in *Military Communications Conference, 2009. MILCOM 2009. IEEE*, 2009, pp. 1-7.

[8] A. Razaque and K. M. Elleithy, "Energy-Efficient Boarder Node Medium Access Control Protocol for Wireless Sensor Networks," *Sensors,* vol. 14, pp. 5074-5117, 2014.

[9] David Martins, and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", 2010 IEEE.

[10] Bo Yu and Bin Xiao, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks", In Parallel and Distributed Processing Symposiun, 2007. ISSNIP 2006, 20th International, page 8 pp., 2006.

[11] Tran Hoang Hai and Eui-Nam Huh, "Detecting Selective Forwarding Attacks in Wireless Sensor Networks Using Two-hops Neighbor Knowledge" Seventh IEEE Internation Symposium on Network Computing and Applications, 2008, pp.325-331.

[12] Huijuan Deng, Xingming Sun, Baowei Wang, Yuanfu Cao, "Selective Forwarding Attack Detection using Watermark in Wireless Sensor Networks", International Colloquium on Computing, Communications Control, and Management (2009 ISECS), pp. 109-113.

[13] Chanatip Tumrongwittayapak and Ruttikorn Varakulsiripunth, "Detecting Sinkhole Attack and Selective Forwarding Attack in Wireless Sensor Networks", ICICS 2009.